KASOWITZ, BENSON, TORRES & FRIEDMAN LLP

1633 BROADWAY
NEW YORK, NEW YORK 10019-6799
212-506-1700
FACSIMILE: 212-506-1800

ATLANTA
HOUSTON
MIAMI
NEWARK
SAN FRANCISCO
SILICON VALLEY

ROBIN L. COHEN
DIRECT DIAL: 212-506-1770
RCOHEN@KASOWITZ.COM

January 13, 2015

VIA EMAIL AND FEDEX
Michael A. Maillet, Esq.
New York Specialty Claims
Chubb Group of Insurance Companies
55 Water Street, 29th Floor
New York, New York 10041
mmaillet@chubb.com

Re:	Company:	Federal Insurance Company
	Insured:	Medidata Solutions, Inc.
	Policy No.:	8212-1392
	Your Claim No.:	339763
	Matter:	Medidata Solutions, Inc.-Crime Loss

Dear Michael:

We have been retained by your insured, Medidata Solutions, Inc. ("Medidata"), in connection with its claim for coverage under Federal Insurance Company ("Federal") Policy No. 8212-1392 (the "Policy") for the loss Medidata sustained as a result of a fraud on or about September 18, 2014 (the "Claim"). Please direct all future communications regarding the Claim to this firm.

Contrary to the position asserted in your December 24, 2014 letter (the "December 24 Letter"), multiple insuring agreements of the Policy apply to the Claim. The most directly applicable coverage grant is the Policy's Computer Fraud Coverage. The insuring agreement for the Computer Fraud Coverage states that "The Company shall pay the **Parent Organization** for direct loss of **Money, Securities** or **Property** sustained by an **Organization** resulting from **Computer Fraud** committed by a **Third Party**." Computer Fraud is defined as: "[T]he unlawful taking or fraudulently induced transfer of **Money, Securities** or **Property** resulting from a **Computer Violation**." It is not disputed that the September 18 wire transfer was fraudulently induced, that Medidata, an "**Organization**" under the Policy, sustained a direct loss of money, or that the perpetrators of the fraud met the Policy definition of a "**Third Party**."

The availability of coverage thus turns on whether there was a "**Computer Violation**," which includes both "the fraudulent (a) entry of **Data** into . . . a **Computer System**; [and] (b) change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format . . . directed against an **Organization**." **Data** is broadly defined under the

Policy, including any "representation of information." The "From" line of an email is a representation of information, i.e. the identity of the sender. By doctoring the "From" line of emails so that the emails appeared to be from Medidata [redacted], the perpetrators fraudulently entered "**Data**" and/or changed "**Data** elements" as required by the Policy. Because that "**Data**" was displayed on computers belonging to Medidata and used by its employees, the Policy definition of "**Computer System**," which includes "a computer and all input, output, processing, storage, off-line media library and communication facilities . . . owned . . . by an **Organization**," is satisfied as well. The facts of the Claim therefore present a "**Computer Violation**," under either prong (a) or (b) of the definition, and the Claim falls squarely within the Computer Fraud Coverage.

In the December 24 Letter you opine that the Claim is not covered under the Computer Fraud Coverage of the Policy because "there was no fraudulent entry of **Data** into Medidata's **Computer System**." This position ignores the inclusion of "representation of information" in the Policy's "**Data**" definition. In the December 24 Letter even you acknowledged that the fraudulent emails contained "false information," which satisfies the definition.

In the December 24 Letter you further state that there is no Computer Fraud Coverage because while the emails included "fictitious" content, "the entry of those emails into the **Computer System** was authorized." This is, in the first instance, contrary to the facts of the Claim – the perpetrators of the fraud manipulated Medidata's email system and created an email on employee computers that was completely unauthorized. Further, this misconstrues what is required by the Computer Fraud Coverage. Here the "**Data**," that is, the "representation of information," that was fraudulently entered was the name of the email sender in the "From" line of the emails. That is the "fraudulent entry of **Data**" or "fraudulent change to **Data** elements" that the Policy requires. The fact that the misrepresented information arrived on Medidata's computers via an inbox to which anyone could send emails is immaterial to the determination of coverage under the Policy. Fraud is often perpetrated by sending false instructions through the mail, over wire, or, in modern times, through email. To bar coverage for this Claim simply because the fraudulent emails were sent to an inbox open to the general public would mean Medidata paid a substantial premium but was still exposed to a wide variety of fraudulent schemes.

In addition, there is also coverage for the Claim under the Policy's Funds Transfer Fraud Coverage. Funds Transfer Fraud is defined as: "[F]raudulent electronic . . . instructions . . . purportedly issued by an **Organization**, and issued to a financial institution directing such institution to transfer, pay or deliver **Money** or **Securities** from any account maintained by such **Organization** at such institution, without such **Organization's** knowledge or consent."

In the December 24 Letter you provide three reasons why the Funds Transfer Fraud Coverage does not apply: (1) The fraudulent instruction was sent to Medidata, not a financial institution; (2) the financial institution in this case received its wire instructions from Medidata, not an entity purporting to be Medidata; and (3) because the wire instructions came from

Medidata, the funds were wired with Medidata's knowledge and consent. Your position ignores the true nature of fraud. When the Medidata employee who initiated the transfers received the doctored emails and believed they were from Medidata's [redacted], the employee became an unwitting participant in the fraud and from that point on expressed the instructions of the members of the fraud, not Medidata.

Viewing the sequence of events in the actual context, a fraudulent instruction was sent to a financial institution when it was relayed by the employee to the bank. The financial institution did not receive authorized instructions from Medidata, because the employee was no longer acting in Medidata's interests. As Medidata was not involved in any acquisition and did not want these funds transferred, of course the funds were not wired with Medidata's knowledge and consent – the funds were wired with the knowledge and consent of a Medidata employee who was unwittingly assisting a fraud.

Finally, the Claim is also covered under the Forgery Coverage. The Forgery Coverage insuring clause provides: "The Company shall pay the **Parent Organization** for direct loss sustained by an **Organization** resulting from **Forgery** or alteration of a **Financial Instrument** committed by a **Third Party**" and provides a non-exclusive list of examples. In the December 24 Letter you state that "the insuring clause requires that the **Forgery** be on a **Financial Instrument**." This reading is not unambiguously supported by the language of the Policy; under the insuring agreement, either a "**Forgery**" *or* an "alteration of a **Financial Instrument**" is sufficient, on its own, for there to be Forgery Coverage. Even if your interpretation of the insuring agreement was reasonable, the Policy would be ambiguous and construed in favor of the insured.

There was a Forgery in this case. "**Forgery**" is defined as "the signing of the name of another natural person . . . with the intent to deceive . . . . Mechanically or electronically produced or reproduced signatures shall be treated the same as hand-written signatures." A perpetrator of the fraud wrote several emails pretending to be Medidata [redacted], with the intent to deceive a Medidata employee into a fraudulent transfer of funds, and electronically signed those emails [redacted]. That forgery, on its own, was sufficient to trigger Forgery Coverage for this Claim.

Medidata fell victim to a classic fraudulent scheme in which a company employee is tricked into thinking she is working to carry out instructions from her employer but instead has been co-opted into a fraud and instead is working for the benefit of those perpetrating the fraud. Medidata specifically purchased insurance from Federal to protect it from exactly this type of fraudulent scheme. Federal has seized on components of the fraud present because it was conducted via email and attempted to fashion those elements into a complete denial of coverage for a Claim that is in fact covered under multiple different coverages in the Policy. In accordance with Federal's obligation to act in good faith and deal fairly with its insured,

Medidata requires acknowledgement of coverage for the Claim and immediate payment of the amount of the loss in excess of the Self-Insured Retention. If you do not retract your denial by January 30, 2015, Medidata reserves the right to take any action, including filing a lawsuit, necessary to redress its claims. Should you have any questions, please do not hesitate to contact us.

Very truly yours,

Robin L. Cohen

cc: Michael Otner (via email – motner@mdsol.com)